UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF FLORIDA

MIAMI DIVISION

Case No. _____

JOHN MCMAHON, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. LAKEVIEW LOAN SERVICING, LLC, Defendant.	CLASS ACTION **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff John McMahon ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through his attorneys, upon personal knowledge as to him and his own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint ("Complaint") against Defendant Lakeview Loan Servicing, LLC ("Lakeview" and/or "Defendant") to hold Defendant accountable for the harm it caused Plaintiff and over 2.5 million similarly situated people ("Class Members"), from its failure to properly secure and safeguard its customers' sensitive personally identifiable

information ("PII"),[1] including their names, addresses, loan numbers and Social Security numbers, and potentially information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

2. In early December 2021, Lakeview discovered that an unauthorized threat actor gained access to its file servers. Upon further investigation, Lakeview determined that the unauthorized threat actor obtained access to files on Lakeview's server for at least almost a month and a half, from October 27, 2021 to December 7, 2021, which included Plaintiff's and Class Members' sensitive PII (the "Data Breach").[2]

3. In mid-March 2022, almost five months after Lakeview believes the Data Breach began, Lakeview finally started sending Data Breach incident letters to Plaintiff and Class Members. Lakeview also sent templates of the Data Breach incident letters to state attorneys general including the Maine Attorney General. The notification sent to the Maine Attorney General identified that approximately 2,537,261 individuals like Plaintiff had their PII accessed,

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR §200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII is also generally defined to include certain identifiers that do not on their face name an individual, but are also considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, and/or financial account number).

[2] Lakeview's Incident Notification Letter sent to the New Hampshire Office of the Attorney General dated March 18, 2022, https://www.doj.nh.gov/consumer/security-breaches/documents/lakeview-loan-servicing-20220318.pdf. While Lakeview's Letter indicated the time period during which the Data Breach occurred, further investigation may reveal a longer Breach period.

exfiltrated, and/or compromised by the Data Breach.[3] Lakeview also reported the Data Breach to the California Attorney General's Office.[4]

4. Upon information and belief, the Data Breach occurred because Lakeview failed to implement adequate and reasonable cyber-security procedures and protocols to protect the PII of Plaintiff and Class Members. Indeed, the deficiencies in Lakeview's data security protocols and practices were so significant that unauthorized person(s) were able to access, view, and/or exfiltrate Plaintiff's and Class Members' PII that can be made available for sale on the illegal marketplace known as the "dark web." In its letter to the New Hampshire Attorney General, Lakeview acknowledged that it was compelled to enhance its then existing cybersecurity measures thereby underscoring that its cybersecurity measures that existed at the time of and during the Data Breach were inadequate and operated in such a manner that permitted the Data Breach to occur.[5]

5. Lakeview has a duty to safeguard and protect customer information entrusted to it and could have prevented the Data Breach had it maintained adequate data security measures and protocols to secure and protect their customers' data.

---

[3] OFF. OF ME. ATT'Y GEN., *Data Breach Notifications*, https://apps.web.maine.gov/online/aeviewer/ME/40/3d0c184e-e78c-4123-8ce8-8535f71facd3.shtml (last visited Mar. 30, 2022).

[4] CAL. DEP'T OF JUST., Rob Bonta Att'y Gen., *Submitted Breach Notification Sample*, https://oag.ca.gov/ecrime/databreach/reports/sb24-551822 (last visited Mar. 30, 2022). The information exposed in the Data Breach was unencrypted. California law requires companies to notify California residents "whose ***unencrypted*** personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security system[.] Cal. Civ. Code §1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data Breach on March 18, 2022.

[5] Lakeview's Incident Notification Letter, *supra* note 2.

6. Lakeview did not adequately safeguard Plaintiff's PII, and now Plaintiff, along with millions of other Class Members, are the victims of a significant Data Breach that, among other harms, puts them at an imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and likely many other Class Members have received notification after the Data Breach that their PII is now available on the Dark Web.

7. Lakeview is responsible for this Data Breach through its failure to implement and maintain adequate and reasonable data security safeguards, and failure to comply with industry-standard data security practices and federal and state laws and regulations governing data security and privacy, including security of PII.

8. Despite its role in managing so much sensitive and personal PII, Lakeview failed to timely recognize and detect unauthorized access and use of its systems, and failed to timely recognize the substantial amounts of data that had been compromised.

9. Lakeview failed to, among other things: timely detect that any unauthorized actors had accessed its file servers; notice the massive amounts of data that were compromised and accessed; and take any steps to investigate the red flags that should have warned Lakeview that its systems were not secure. Had Lakeview properly maintained and monitored its information technology infrastructure and denied access to that infrastructure to potential threats, it would have either prevented the Data Breach altogether or at the very least discovered the invasion sooner.

10. Lakeview owed statutory, regulatory, and common law duties to Plaintiff and Class Members to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access. Lakeview was and remains required to maintain the security and privacy of the PII entrusted to them. When Plaintiff and Class Members provided their PII, Lakeview was required

to comply with the obligation to keep Plaintiff's PII secure and safe from unauthorized access, to use this information for business purposes only, and to make only authorized disclosures of this information.

11. Plaintiff and Class Members entrusted Lakeview with, and allowed Lakeview to gather, highly sensitive information as part of the provision of Lakeview's services. They did so in confidence, and they had the legitimate expectation that Lakeview would respect their privacy and act appropriately.

12. Trust and confidence are key components of Plaintiff's and Class Members' relationship with Lakeview. Without it, Plaintiff and Class Members would not have provided Lakeview with, or allowed Lakeview to collect, their most sensitive information in the first place. To be sure, Plaintiff and Class Members relied upon Lakeview to keep their information secure, as they are required by law to do.

13. In this era of frequent data security attacks and data breaches, Lakeview's failures leading to the Data Breach are particularly egregious.

14. As a result of Lakeview's failures to protect the PII of Plaintiff and Class Members, their PII was accessed and downloaded by one or more unauthorized actors. As a direct and proximate result, Plaintiff and Class Members are now at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

15. Plaintiff's and Class Members' injuries described herein were exacerbated by the over four-month delay in informing and notifying Plaintiff and Class Members of the Data Breach

and the theft of their PII. Plaintiff and Class Members were unable to take actions to protect themselves and attempt to mitigate the harm until they received notice.

16. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (e) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals and made available on the Dark Web; (f) damages to and diminution in value of their personal data; (g) the reasonable value of the PII; (h) actual damages in the form of the difference in value between the services that should have been delivered and the services that were actually delivered; and (i) the continued risk to their PII, which remains in the possession of Lakeview, and which is subject to further breaches, so long as Lakeview fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII; and (j) intrusion about into their private lives.

17. Plaintiff seeks to remedy these harms, and to prevent their future occurrence, on behalf of himself and all similarly situated persons whose PII was compromised as a result of the Data Breach.

18. Accordingly, Plaintiff, on behalf of himself and Class Members, assert claims for negligence, negligence *per se,* breach of contract, breach of implied contract, breach of confidence, intrusion upon seclusion, violation of the Florida Deceptive and Unfair Trade Practices Act, Fla.

Stat. §§501.201, *et seq*. ("FDUTPA"), and violation of the Maryland Consumer Protection Act, Md. Code Com. Law Section 13-101, *et seq*. Plaintiff and Class Members seek declaratory and injunctive relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Defendant Lakeview Loan Servicing, LLC

19. Defendant Lakeview is a Delaware limited liability company with its principal place of business in Coral Gables, Florida. According to Lakeview's filings with the Florida Department of State, all members of Lakeview as a limited liability company are residents and citizens of Florida and have an apparent intention to remain domiciled in Florida.

20. Lakeview touts itself as the Fourth Largest Mortgage Servicer in the United States and claims to work with more than 1.4 million customers annually with their mortgages. Lakeview's website states that its "in house team of mortgage loan experts is focused on assisting our customers with new home financing. Whether you're interested in purchasing a new home, or simply want to explore restricting your current financing, we're here to help! We might be able to lower your monthly payment, help you to consolidate your other debt, or give you cash to use however you'd like."[6]

Plaintiff John McMahon

21. Plaintiff John McMahon is a citizen of Maryland residing in Bel Air, Maryland. He intends to remain a citizen of Maryland. In late March 2022, Plaintiff received a letter from Lakeview dated March 16, 2022 notifying him of the Data Breach. The letter unequivocally states

[6] LAKEVIEW, *About*, https://lakeview.com/about/ (last visited Mar. 30, 2022).

that Plaintiff's PII was accessed in the Data Breach: "On January 1, 2022, the review process generated a preliminary list of individuals, including you, whose name, address, loan number and Social Security number were included in the files" that were accessed by the unauthorized actor during the Data Breach.

JURISDICTION & VENUE

22. This Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. §1332(d)(2), because this is a putative class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, Plaintiff, many absent Class Members,[7] and Lakeview are citizens of different states. Plaintiff is a citizen of Maryland and the members of Lakeview as a limited liability company are citizens of Florida thereby satisfying CAFA's minimal diversity requirement.

23. This Court has general personal jurisdiction over Lakeview because its principal place of business is located in this district at 4425 Ponce de Leon Boulevard, Coral Gables, FL 33146.

24. Venue is proper in this district under 28 U.S.C. §§1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, Lakeview conducts substantial business in this district, and is located in this district. On information and belief, Plaintiff's and Class Members' PII was transmitted to and by Lakeview and inputted into its network within this district. Lakeview is

[7] While Lakeview services mortgages for Floridians, Plaintiff and other Class Members outside Florida were impacted, including 9,511 residents of Maine. OFF. OF ME. ATT'Y GEN., *supra* note 3.

based in this district, is believed to maintain Plaintiff's and Class Members' PII in the district and the harm caused to Plaintiff and Class Members emanated from this district.

FACTUAL ALLEGATIONS

Lakeview Acquires, Collects, and Maintains Plaintiff's and Class Members' PII

25. Plaintiff and Class Members have a legal and equitable relationship with Lakeview as Lakeview services on their mortgage loans. As part of the servicing relationship, Plaintiff and Class Members were required to provide their sensitive PII to Lakeview.

26. Lakeview, in its Privacy Policy, promised to protect Plaintiff's and Class Members' PII.[8] Despite the representations in the Privacy Policy, Lakeview failed to protect Plaintiff's and Class Members' PII because an unauthorized actor accessed Plaintiff's and Class Members' PII during the Data Breach without their consent.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII, Lakeview owes legal and equitable duties to those individuals and was responsible for protecting Plaintiff's and Class Members' PII from disclosure and unauthorized access.

28. Lakeview was required to keep Plaintiff's and Class Members' PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

[8] LAKEVIEW, *Privacy Policy*, https://lakeview.com/privacy-policy/ (last visited Mar. 30, 2022) ("To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.).

The Data Breach

29. According to Defendant, an unauthorized person obtained access to files on Lakeview's file storage servers from October 27, 2021 to December 7, 2021. Defendant has further disclosed that these files contained, at the very least, victims' names, addresses, loan numbers, and Social Security numbers.

30. Upon information and belief, the data accessed in the Data Breach was then exfiltrated and sold or made available on the dark web. For example, on January 25, 2022, Plaintiff received a notification from his credit monitoring service that on January 24, 2022, his Social Security number was located on the dark web.

31. The Data Breach notices sent to Plaintiff and Class Members offered them a one-year membership to credit monitoring services. This is wholly inadequate because victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft. Defendant even acknowledges this in its sample notification letters provided to states' Attorneys General, which instruct victims of the Data Breach to "be vigilant for incidents of fraud or identity theft … over the next 12 to 24 months."[9]

32. The Data Breach notification letters sent to Plaintiff and Class Members also suggested several additional time consuming steps that Plaintiff and Class Members could take to protect themselves moving forward as a result of the Data Breach, such as fraud alerts, credit freezes, and/or contacting government authorities.

[9] *See, e.g.*, LAKEVIEW, *Notice of Data Breach*, https://oag.ca.gov/system/files/Lakeview%20-%20California%20Notification.pdf (last visited Mar. 30, 2022).

33. Based on Lakeview's urging Plaintiff and Class Members to take these mitigating actions, as well as its decision to provide victims with credit monitoring services, it is abundantly clear that the perils from the Data Breach are real and concrete, and not hypothetical or attenuated.

34. Despite all of the publicly available knowledge of the continued compromises of PII, Lakeview's approach to maintaining the privacy of Plaintiff's and Class Members' PII was inadequate, unreasonable, negligent, and reckless. This is evidenced by Lakeview's Data Breach notice, wherein Lakeview stated in response to the Data Breach that "[a]dditional steps are being taken to further enhance our existing security measures."[10] Implied in Lakeview's statement is an admission that Lakeview's technical and cybersecurity capabilities were inadequate, which resulted in the Data Breach and the divulgence of Plaintiff's and Class Members' PII.

35. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

[10] *Id.*

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

36. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you

know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[11]

37. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

[11] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (original release date Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

Monitor for adversarial activities
Hunt for brute force attempts
Monitor for cleanup of Event Logs
Analyze logon events;

Harden infrastructure

Use Windows Defender Firewall
Enable tamper protection
Enable cloud-delivered protection
Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[12]

38. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

[12] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT SECURITY, (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

39. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members. Moreover, given Defendant's notification to the California Attorney General, it is clear that Defendant failed to encrypt the PII on its network and systems, which was negligent in and of itself. Had the PII been encrypted, the threat actors would not be able to read any of the PII.

Defendant Knew or Should Have Known of the Risk Because the Financial Sector is Particularly Susceptible to Cyber Attacks

40. Defendant knew and understood unprotected or exposed PII in the custody of loan servicing companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

41. Lakeview is fully aware of how sensitive the PII it stores and maintains is. It is also aware of how much PII it collects, uses, and maintains from Plaintiff and Class Members. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled, quickly mitigating the hackers' ability to cause further harm. Instead, types of PII that cannot be easily changed (such as dates of birth and Social Security numbers) are the most valuable to hackers.[13]

[13] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* DONNELLON MCCARTHY ENTERS. (July 21, 2020), https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/.

42. At a Federal Trade Commission ("FTC") public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[14]

43. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

44. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details

---

[14] Transcript, *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[15] 17 C.F.R. §248.201 (2013).

[16] *Id.*

have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

Social Security Numbers Are Particularly Valuable

45. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

46. It is incredibly difficult to change a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual

---

[17] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[18] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[19] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Mar. 30, 2022).

[20] *Identity Theft and Your Social Security Number*, SSA, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 30, 2022).

misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

47. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

48. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, name, and date of birth.

49. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[22]

---

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

[22] Tim Greene, *Anthem Hack: Personal data stolen sells for 10x price of stolen credit card numbers*, NETWORK WORLD (Feb. 6, 2015), https://www. networkworld .com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

50. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

51. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

52. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach. Further, Defendant had a legal duty to safeguard the PII.

53. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

54. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of

[23] Report to Congressional Requesters, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

55. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[24] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[25]

56. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[26] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed[,] 69 percent reported feelings of fear related to personal financial safety[,] 60 percent reported anxiety[,] 42 percent reported fearing for the financial security of family members[, and] 8 percent reported feeling suicidal."[27]

---

[24] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.justice.gov/usao-wdmi/file/764151/download.

[25] *See id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. §603.2(a). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 16 C.F.R. §603.2(b)

[26] Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, NORTONLIFELOCK (Feb. 4, 2021), https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html.

[27] *Id.* (citing *Identity Theft: The Aftermath 2016™*, IDENTITY THEFT RES. CTR. (2016) https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf).

57. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

58. The FTC has brought enforcement actions against businesses for failing to protect consumers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. §45.

59. Identity thieves may commit various types of crimes such as, *inter alia*, immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, fraudulently obtaining medical services, and/or using the victim's information to obtain a fraudulent tax refund.

60. The United States government and privacy experts acknowledge that it may take much time for identity theft to come to light and be detected because identity thieves may wait years before using the stolen data.

61. Because the information Lakeview allowed to be compromised and taken is of such a durable and permanent quality (*i.e.*, name, address, lean number, and Social Security number), the harms to Plaintiff and the Class will continue and increase, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

Lakeview's Post-Breach Activity Was (and Remains) Inadequate.

62. Immediate notice of a security breach is essential to protect victims such as Plaintiff and Class Members. Plaintiff and Class Members here did not receive notice of the Data Breach

until more than three months after the Data Breach was discovered, thus further exacerbating the harm Plaintiff and Class Members suffered as a result of the Data Breach.

63. Plaintiff and Class Members have suffered real and tangible losses, including but not limited to the loss in the inherent value of their PII, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but until recently, kept silent by Lakeview.

64. Despite Lakeview's failure to protect Plaintiff's and Class Members' PII and the persistent nature of the PII exposed, Lakeview has only offered to provide Plaintiff and Class Members with one year of credit monitoring.

65. As a result of the Lakeview's failure to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII are used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. The continued risk to their PII that is subject to further breaches so long as Lakeview fails to undertake appropriate measures to protect the PII in Lakeview's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

66. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable and continuing interest in ensuring that their PII that remains in the possession of Lakeview is secure, remains secure, and is not subject to further theft.

Plaintiff John McMahon's Experience

67. Plaintiff was required to provide and did provide his PII in connection with obtaining the mortgage serviced by Defendant. The PII included, but was not limited to, his name, address, Social Security number, and tax information.

68. The notice letter about the Data Breach admits Plaintiff's PII was accessed in the Data Breach. The letter also states that Defendant knew about this on January 31, 2022, but did not take steps to inform Plaintiff until mailing him a letter on or about March 16, 2022, which Plaintiff did not actually receive until on or about March 28, 2022.

69. On January 25, 2022, roughly two months before receiving the notification from Defendant, Plaintiff was informed by Discover, through which he has credit monitoring services,

that his Social Security number was "compromised." The alert further stated: "We have located your Social Security number on a Dark Web site."

70. Plaintiff stores any documents containing his PII in a safe and secure location. And he diligently chooses unique usernames and passwords for his online accounts.

71. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. He also spent considerable time implementing an alert with one of the major credit bureaus, and intends to spend time taking steps to protect his PII with the other major credit bureaus as well. This is time that was and will be lost and unproductive and taken away from other activities and duties.

72. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

73. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

74. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals.

75. As a result of the Data Breach and the placement of his Social Security number on the dark web, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

76. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach. It offered identity monitoring services, but only for one year.

Defendant Violated the Gramm-Leach-Bliley Act

77. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §6809(3)(A), and thus is subject to the GLBA.

78. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. §6809(3)(A).

79. Defendant collects nonpublic personal information, as defined by 15 U.S.C. §6809(4)(A), 16 C.F.R. §313.3(n) and 12 C.F.R. §1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§6801.1 *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. §1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

80. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

81. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and

conspicuous." 16 C.F.R. §§313.4 and 313.5; 12 C.F.R. §§1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. §313.3(b)(1); 12 C.F.R. §1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. §313.4 and 313.5; 12 C.F.R. §§1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. §313.6; 12 C.F.R. §1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. §313.9; 12 C.F.R. §1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

82. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network.

83. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

84. The Safeguards Rule, which implements Section 501(b) of the GLBA,15 U.S.C. §6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating

one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

85. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control.

86. Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

87. Defendant failed to adequately oversee service providers.

88. Defendant failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Defendant Violated the FTC Act

89. Section 5 of the FTC Act, 15 U.S.C. §45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice

by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

90. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

CLASS ACTION ALLEGATIONS

91. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff seeks to bring this class action on behalf of himself and a nationwide class (the "Nationwide Class") defined as follows:

> **All natural persons residing in the United States whose Personal Information was compromised in the Data Breach.**

92. Plaintiff also seeks to certify the following subclass:

> **Florida Subclass: All natural persons who reside in Florida whose PII was compromised in the Data Breach.**
>
> **Maryland Subclass: All natural persons who reside in Maryland whose PII was compromised in the Data Breach.**

93. Excluded from the Class are Lakeview; its officers, directors, and employees of Lakeview; any entity in which Lakeview has a controlling interest, is a parent or subsidiary, or which is controlled by Lakeview; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Lakeview. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

94. Plaintiff reserves the right to modify and/or amend the Nationwide Class and the Maryland Subclass definitions, including but not limited to creating additional subclasses, as necessary.

95. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

96. All Class Members are readily ascertainable in that Lakeview has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

97. ***Numerosity***. Consistent with Fed. R. Civ. P. 23(a)(1), the Nationwide Class and the Maryland Subclass are so numerous that joinder of all members is impracticable. While the exact number of Nationwide Class Members is unknown, upon information and belief, it is in excess of two million, and the Maryland Subclass more than likely contains at least 50 individuals.

98. ***Commonality and Predominance***. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

a. whether Lakeview engaged in the wrongful conduct alleged in this Complaint;

b. whether Lakeview's conduct was unfair, unconscionable, and/or unlawful;

c. whether Lakeview failed to implement and maintain adequate and reasonable systems and security procedures and practices to protect Plaintiff's and Class Members' PII;

d. whether Lakeview owed a duty to Plaintiff and Class Members to adequately protect their PII and to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

e. whether Lakeview breached its duties to protect the PII of Plaintiff and Class Members by failing to provide adequate data security and failing to provide appropriate and adequate notice of the Data Breach to Plaintiff and Class Members;

f. whether Lakeview's conduct was negligent;

g. whether Lakeview knew or should have known that its computer systems were vulnerable to being compromised;

h. whether Lakeview's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Plaintiff's and Class Members' PII;

i. whether Lakeview wrongfully or unlawfully failed to inform Plaintiff and Class Members that it did not maintain computers and security practices adequate to reasonably safeguard Plaintiff's and Class Members' PII;

j. whether Plaintiff and Class Members suffered injury, including ascertainable losses, as a result of Lakeview's conduct (or failure to act);

k. whether Plaintiff and Class Members are entitled to recover damages; and

l. whether Plaintiff and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

99. ***Typicality***. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the misconduct of Lakeview, described in this Complaint, and assert the same claims for relief.

100. ***Adequacy***. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff is a member of the Class he seeks to represent; are committed to pursuing this matter against Lakeview to obtain relief for the Class; and have no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiff retained counsel who are competent and experienced in litigating class actions and complex litigation, including privacy litigation of this kind. Plaintiff and his counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

101. ***Superiority***. Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Lakeview's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Lakeview's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Lakeview's conduct and/or inaction.

Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

102. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the common questions of law or fact predominate over any questions affecting individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

103. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Lakeview. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Lakeview to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

104. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Lakeview, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Lakeview continues to maintain its inadequate security practices, retain

possession of Plaintiff's and Class Members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

105. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Plaintiff's and Class Members' PII were accessed, compromised, or stolen in the Data Breach;

b. whether Lakeview owed a legal duty to Plaintiff and the Class Members;

c. whether Lakeview failed to take adequate and reasonable steps to safeguard the PII of Plaintiff and Class Members;

d. whether Lakeview failed to adequately monitor its data security systems;

e. whether Lakeview failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Lakeview knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiff's and Class members' PII secure; and

g. whether Lakeview's adherence to FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

106. Plaintiff incorporates paragraphs 1-105 of the Complaint as if fully set forth herein.

107. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

108. Lakeview collected, stored, used, and benefited from the non-public PII of Plaintiff and Class Members in the provision of servicing mortgages on Plaintiff's and Class Members' properties.

109. Lakeview had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if their PII were wrongfully disclosed.

110. By collecting, storing, and using Plaintiff's and Class Members' PII, Lakeview owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII. Lakeview owed a duty to prevent the PII it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

111. Lakeview was required to prevent foreseeable harm to Plaintiff and Class Members, and it therefore had a duty to take adequate and reasonable steps to safeguard its sensitive PII from unauthorized release or theft. This duty included: (1) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiff's and Class Members' PII in its possession was adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of

the PII of Plaintiff and Class Members; and (4) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

112. Lakeview had a common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices of Defendant in its collection, storage, and use of PII from Plaintiff and Class Members. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because malicious actors routinely attempt to steal such information for use in nefarious purposes, but Defendant also knew that it was more likely than not Plaintiff and Class Members would be harmed as a result.

113. Lakeview's obligation to use adequate and reasonable security measures also arose as a result of the special relationship that existed between it, on the one hand, and Plaintiff and Class Members, on the other hand. This special relationship arose because Defendant collected, stored, and used the PII of Plaintiff and Class Members for the procurement and provision of financial services for Plaintiff and Class Members. Defendant alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

114. Additionally, the policy of preventing future harm weighs in favor of finding a special relationship between Lakeview and Plaintiff and Class Members. If companies are not held accountable for failing to take adequate and reasonable security measures to protect the sensitive PII in its possession, they will not take the steps that are necessary to protect against future security breaches.

115. Defendant also owed a duty to timely disclose the material fact that its computer systems and data security practices and protocols were inadequate to safeguard users' personal and financial data from theft.

116. The injuries suffered by Plaintiff and Class Members were proximately and directly caused by Lakeview's failure to follow reasonable, industry standard security measures to protect Plaintiff's and Class Members' PII.

117. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

118. If Defendant had implemented the requisite, industry standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII of Plaintiff and Class Members.

119. Defendant breached these duties through the conduct alleged here in this Complaint by, including without limitation, failing to protect the PII in its possession; failing to maintain adequate computer systems and allowing unauthorized access to and exfiltration of Plaintiff's and Class Members' PII; failing to disclose the material fact that Lakeview's computer systems and data security practices were inadequate to safeguard the PII in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiff and Class Members the material fact of the Data Breach.

120. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised. And as a direct and proximate

result of Defendant's failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII of Plaintiff and Class Members were accessed by ill-intentioned individuals who could and will use the information to commit identity or financial fraud. Plaintiff and Class Members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

121. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII of current and former borrowers and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members.

122. It was foreseeable that Defendant's failure to exercise reasonable care to safeguard the PII in its possession or control would lead to one or more types of injury to Plaintiff and Class Members. And the Data Breach was foreseeable given the known, high frequency of cyberattacks and data breaches in the financial industry.

123. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of PII, the current cyber scams being perpetrated on PII, and that it had inadequate protocols, including security protocols in place to secure the PII of Plaintiff and Class Members.

124. Defendant's own conduct created the foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included its failure to take the steps and opportunities to prevent the Data Breach and its failure to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

125. Plaintiff and Class Members have no ability to protect their PII that was and is in Defendant's possession. Defendant alone was and is in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

126. As a direct and proximate result of Lakeview's negligence as alleged above, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII is used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. The continued risk to their PII that is subject to further breaches so long as Lakeview fails to undertake appropriate measures to protect the PII in Lakeview's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

127. Pursuant to the FTC Act, 15 U.S.C. §45, Lakeview had a duty to provide fair and adequate computer systems and data security measures to safeguard the PII of Plaintiff and Class Members.

128. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Lakeview's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

129. Pursuant to the Gramm-Leach-Bliley Act, Lakeview had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. §6801.

130. Pursuant to the Fair Credit Reporting Act ("FCRA"), Lakeview had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. §1681(b).

131. Lakeview solicited, gathered, and stored PII of Plaintiff and Class Members to facilitate transactions which affect commerce.

132. Lakeview violated the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein.

Lakeview's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Lakeview's systems.

133. Lakeview's violation of the FTC Act (and similar state statutes) as well as its violations of the FCRA, and the Graham-Leach-Bliley Act constitutes negligence.

134. Plaintiff and Class Members are within the class of persons that the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act were intended to protect.

135. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act (and similar state statutes), as well as the FCRA, and the Graham-Leach-Bliley Act, were intended to guard against. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ adequate and reasonable data security measures, caused the same harm as that suffered by Plaintiff and Class Members.

136. As a direct and proximate result of Lakeview's violations of the above-mentioned statutes (and similar state statutes), Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT II

NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class)

137. Plaintiff incorporates paragraphs 1-105 of the Complaint as if fully set forth herein.

138. Pursuant to the FTC Act, 15 U.S.C. §45, Lakeview had a duty to provide fair and adequate computer systems and data security measures to safeguard the PII of Plaintiff and Class Members.

139. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Lakeview's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

140. Pursuant to the Gramm-Leach-Bliley Act, Lakeview had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. §6801.

141. Pursuant to the FCRA, Lakeview had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. §1681(b).

142. Lakeview solicited, gathered, and stored PII of Plaintiff and Class Members to facilitate transactions which affect commerce.

143. Lakeview violated the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein. Lakeview's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Lakeview's systems.

144. Lakeview's violation of the FTC Act (and similar state statutes) as well as its violations of the FCRA, and the Graham-Leach-Bliley Act constitutes negligence per se.

145. Plaintiff and Class Members are within the class of persons that the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act were intended to protect.

146. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act (and similar state statutes), as well as the FCRA, and the Graham-Leach-Bliley Act, were intended to guard against. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ adequate and reasonable data security measures, caused the same harm as that suffered by Plaintiff and Class Members.

147. As a direct and proximate result of Defendant's negligence per se under the FTC Act, Plaintiff and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT III

BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclasses)

148. Plaintiff incorporates paragraphs 1-105 of the Complaint as if fully set forth herein.

149. Plaintiff and Class Members maintained a confidential relationship with Defendant whereby Defendant undertook a duty not to disclose the PII provided by Plaintiff and Class Members to Defendant to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

150. Defendant knew Plaintiff's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

151. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred

because Defendant failed to implement and maintain reasonable safeguards to protect the PII in their possession and failed to comply with industry-standard data security practices.

152. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

153. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT IV

INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Nationwide Class)

154. Plaintiff incorporates paragraphs 1-105 of the Complaint as if fully set forth herein.

155. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party that was unequipped and unable to keep their PII secure.

156. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

157. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential.

158. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT V

Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. §§501.201, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class)

159. Plaintiff incorporates paragraphs 1-105 of the Complaint as if fully set forth herein.

160. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

161. This cause of action is brought pursuant the FDUTPA, which, pursuant to Fla. Stat. §501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

162. Lakeview's offer, provision, and sale or services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§501.201-501.213.

163. Plaintiff and the Class Members, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. §501.203(7).

164. Lakeview serviced loans obtained by Plaintiff and the Class Members.

165. Lakeview offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. §501.203.

166. Plaintiff and the Class Members paid for or otherwise availed themselves and received services from Lakeview, primarily for personal, family, or household purposes.

167. Lakeview engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiff and Class Members.

168. Lakeview's acts, practices, and omissions were done in the course of Lakeview's business of offering, providing, and servicing loans throughout Florida and the United States.

169. The unfair, unconscionable, and unlawful acts and practices of Lakeview alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

170. Lakeview, headquartered and operating in and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. §501.204(1), including but not limited to the following:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiff's and Class Members' PII;

d. continued acceptance and storage of PII after Lakeview knew or should have known of the security vulnerabilities that were exploited in the Data Breach;

e. continued acceptance and storage of PII after Lakeview knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

171. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. §41, *et seq.*, and the FDUTPA, Fla. Stat. §501.171(2).

172. Lakeview knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data breach or theft was high.

173. Plaintiff has standing to pursue this claim because as a direct and proximate result of Lakeview's violations of the FDUTPA, Plaintiff and Class Members have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that Lakeview's acts or practices violate the FDUTPA. *See* Fla. Stat. §501.211(a).

174. Plaintiff also has standing to pursue this claim because, as a direct result of Lakeview's knowing violation of the FDUTPA, Plaintiff is at a substantial and imminent risk of future identity theft. Lakeview still possesses Plaintiff's and the Class Members' PII, and some

Plaintiff's PII has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiff and Class Members.

175. Plaintiff and Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that Lakeview engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Lakeview's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Lakeview engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Lakeview audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Lakeview segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Lakeview purge, delete, and destroy PII not necessary for its provisions of services in a reasonably secure manner;

f. ordering that Lakeview conduct regular database scans and security checks;

g. ordering that Lakeview routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Lakeview to meaningfully educate individuals about the threats they face as a result of the loss of their financial and PII to third parties, as well as the steps victims should take to protect themselves.

176. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Lakeview's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

177. The above unfair, unconscionable, and unlawful practices and acts by Lakeview were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

178. Lakeview's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

179. Plaintiff and Class Members seek relief under the FDUTPA, Fla. Stat. §§501.201, *et seq.*, including, but not limited to, a declaratory judgment that Lakeview's actions and/or practices violate the FDUTPA; injunctive relief enjoining Lakeview, its employees, parents, subsidiaries, affiliates, executives, and agents from violating the FDUTPA, ordering that Lakeview engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems

on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors, ordering that Lakeview engage third-party security auditors and internal personnel to run automated security monitoring, ordering that Lakeview audit, test, and train security personnel regarding any new or modified procedures, ordering that Lakeview segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system, ordering that Lakeview purge, delete, and destroy PII not necessary for its provisions of services in a reasonably secure manner, ordering that Lakeview conduct regular database scans and security checks, ordering that Lakeview routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach, ordering Lakeview to meaningfully educate individuals about the threats they face as a result of the loss of their financial and PII to third parties, as well as the steps victims should take to protect themselves, and any other just and proper relief.

180. Plaintiff and Class Members are also entitled to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

COUNT VI

Violations of the Maryland Consumer Protection Act,
Md. Code Com. Law Section 13-101, *et seq.*
(On Behalf of Plaintiff and the Maryland Subclass)

181. Plaintiff incorporates paragraphs 1-105 of the Complaint as if fully set forth herein.

182. Plaintiff brings this claim pursuant to the Maryland Consumer Protection Act, Md. Code Com. Law §13-101, *et seq.* ("MCPA").

183. Defendant, Plaintiff, and the Maryland Class are "persons" within the meaning of Md. Code Com. Law §13-101(h).

184. The MCPA provides that a person may not engage in any unfair or deceptive trade practice in the sale of any consumer good. Md. Code Com. Law §13-303.

185. Defendant participated in misleading, false, or deceptive acts that violated the MCPA. Defendant also intentionally concealed and suppressed material facts concerning the Data Breach and its data security practices. The following actions and omissions are examples of Defendant's tortious conduct:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiff's and Class Members' PII;

d. continued acceptance and storage of PII after Lakeview knew or should have known of the security vulnerabilities that were exploited in the Data Breach; and

e. continued acceptance and storage of PII after Lakeview knew or should have known of the Data Breach.

186. Plaintiff and Maryland Subclass members had limited means of discerning that Defendant's representations were false and misleading until after Defendant obtained and

mishandled their PII. Thus, acting reasonably, Plaintiff and Maryland Subclass members did not and could not unravel Defendant's deception.

187. Defendant's actions as set forth above occurred in the conduct of trade or commerce.

RELIEF REQUESTED

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, respectfully requests the following relief:

A. An order certifying this case as a class action on behalf of the Class, defined above, appointing Plaintiff as Class representative and appointing the undersigned counsel as Class counsel;

B. A mandatory injunction directing Lakeview to adequately safeguard Plaintiff's and Class Members' PII by implementing improved security procedures and measures as outlined above;

C. An award of other declaratory, injunctive, and equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. An award of restitution and compensatory, consequential, and general damages to Plaintiff and Class Members, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

E. An award of actual or statutory damages to Plaintiff and Class Members in an amount to be determined at trial or by this Court;

F. An award of reasonable litigation expenses and costs and attorneys' fees to the extent allowed by law;

G. An award to Plaintiff and Class Members of pre- and post-judgment interest, to the extent allowable; and

H. Award of such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

DATED: March 31, 2022

ROBBINS GELLER RUDMAN & DOWD LLP

s/Stuart A. Davidson
STUART A. DAVIDSON

STUART A. DAVIDSON (FBN 0084824)
DOROTHY P. ANTULLIS (FBN 890421)
ERIC S. DWOSKIN (FBN 112459)
MAXWELL H. SAWYER (FBN 1003922)
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
sdavidson@rgrdlaw.com
dantullis@rgrdlaw.com
edwoskin@rgrdlaw.com
msawyer@rgrdlaw.com

MARKOVITS, STOCK & DEMARCO, LLC
TERENCE R. COATES (*pro hac vice forthcoming*)
DYLAN J. GOULD (*pro hac vice forthcoming*)
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 513/651-3700
513/665-0219 (fax)
tcoates@msdlegal.com
dgould@msdlegal.com

Counsel for Plaintiff and the Putative Class